School of

Engineering and Computer Science

Te Kura Mātai Pūkaha, Pūrorohiko

CYBR 171 T1 2023

Ngā whakapūtanga o Te Haumaru rorohiko
Cybersecurity Fundamentals

Key Concepts

Learning objectives

- Understand what we mean by cybersecurity and what is a “secure” system.
- Compare and contrast different types of attackers (also know as adversaries), their motivations and capabilities.
- Understand whether some aspects of the legal and ethics of white hat hacking.

PART I:
What is cybersecurity?

Cybersecurity is …

“a computing-based discipline involving technology, people, information, and processes to enable assured operations.
It involves the creation, operation, analysis, and testing of secure computer systems.
It is an interdisciplinary course of study, including aspects of law, policy, human factors, ethics, and risk management in the context of adversaries”

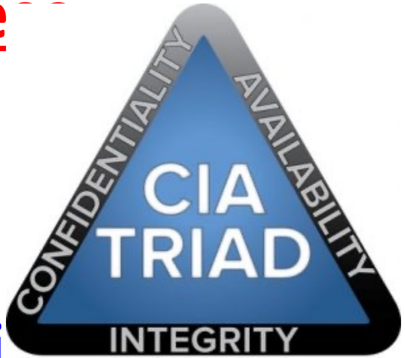
Joint Task Force on Cybersecurity Education (JTF)

https://cybered.hosting.acm.org/wp/about/

Cybersecurity is …

“ the prevention of damage to, unauthorized use of, exploitation of, and—if needed—the restoration of electronic information and communications systems, and the information they contain, in order to **strengthen the confidentiality, integrity and availability of these systems**.”

US National Institute of Standards – Information Technology Laboratory



https://csrc.nist.gov/glossary/term/cybersecurity

The CIA Properties

Confidentiality

- Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information

Integrity

- Guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity

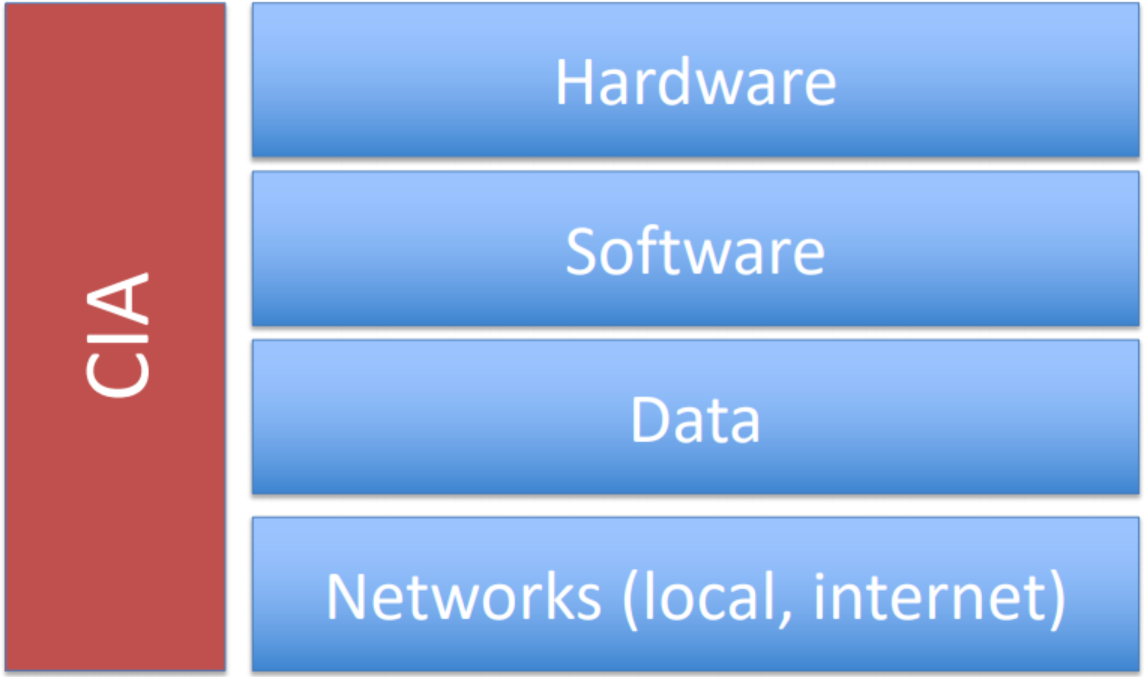
Availability

- Ensuring timely and reliable access to and use of information

CIA
TRIAD
CONFIDENTIALITY
AVAILABILITY
INTEGRITY

System resources or assets

What are we trying to **protect**?



CIA

Hardware

Software

Data

Networks (local, internet)

CIA Examples

- **Confidentiality**:
  - Publishing private data on the web obtained by unauthorized parties (data breach)
  - Monitoring keypresses and sending them to a unauthorized third-party (keylogger)
- **Integrity**
  - Encrypting or scrambling data stored on a drive (ransomware)
  - Changing value of a stock in a financial system to inflate its value (intrusion by a hacker)
  - Alter a website's HTML to vandalize it (defacement)
- **Availability**
  - Preventing legitimate users accessing a website by overloading it with traffic (denial-of-service)
  - Delete files from the hard drive (Chernobyl virus)

Tradeoffs between CIA properties

- Which property is most important depends upon the purpose of the system being protected.
- You may only have limited resources and need to priorities one or two properties over others.
- Examples:
  - Health records systems
  - Financial records
  - Location tracking

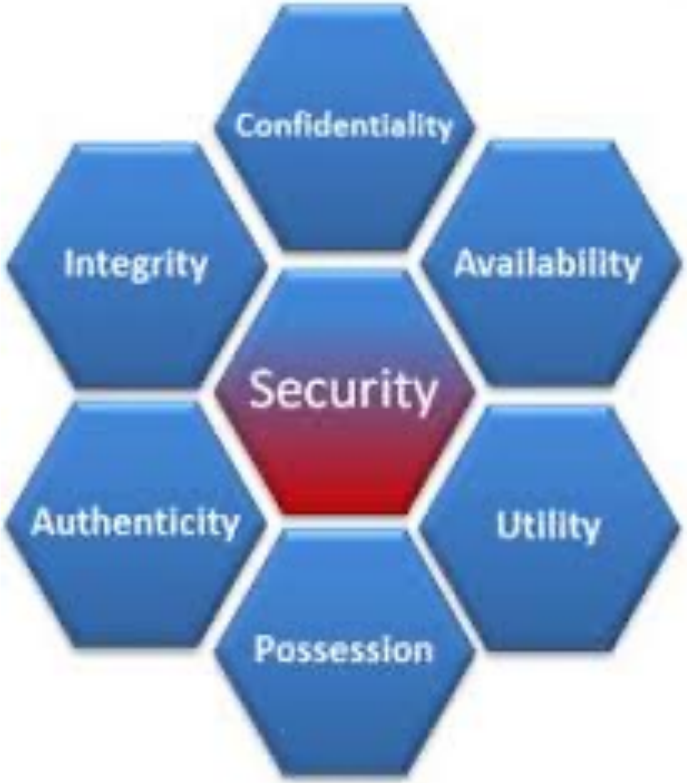
C&I versus A

- Sometimes confidentiality & integrity conflict with availability.
- You need to balance these requirements against each other depending upon context.
- Examples:
  - Multiple systems = high availability but increase burden for implementing confidentiality & integrity
  - 2 factor authentication = better confidentiality & integrity but lower availability

ISO/IEC 27001, an international standard

- **Non-repudiation** – means one party cannot deny receiving a message or a transaction, nor can the other party deny sending a message or a transaction (only Ian could have sent that message)
- **Authenticity** – proving who you are and each input is from a trusted source **(the message was sent by Ian and is genuine)**
- **Accountability** – tracing the actions of an entity uniquely to that entity **(there is a record of who sent the message and controls exist on how that record is updated)**

Parkerian Hexad



Security *policy*

- Security policy is set of rules that should be followed to enforce security policies.
- A security policy might specify:
  - Who (entity)
  - What (operation)
  - Which (system asset)
- Example of policy enforcing confidentiality of an exam such that only Bob may change it (integrity):
  - Alice can read the exam.
  - Bob can read and write to the exam.
  - Carol can print the exam.

Security *mechanism*

- Security policy does not specify how the rules are enforced.
- Might be more than one way to enforce the rules.
- Example of the exam from previous slide:
  - Physical controls limiting access to exam paper.
  - Operating system controls limiting access to exam paper.
  - Cryptographic controls limiting access to exam paper.
- Role of cybersecurity engineer is to decide the best mechanism according to criteria such as time, cost etc.

PART II:
What are we protecting against and how?

Vulnerabilities

- **Weakness** in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
- Examples of vulnerabilities for Internet banking
  - I always use an easy to guess password
  - Internet banking gives anyone access if a longer than expected password is entered
  - I do all of my internet banking using a PC at the local internet cafe

Threats and attacks

- A threat is any circumstance or event with the potential to adversely impact the security properties of an information system
  - events can be intentional or unintentional
  - emphasis on potential effect
- An attack **is an attempt to gain unauthorised** access to system services, resources, or information, or **an attempt to compromise** system integrity, availability, or confidentiality.
  - always intentional in nature
  - exploits a vulnerability that exists in the system
  - successful attack is a threat that has happened

Example threats and attacks

- Examples of vulnerabilities for Internet banking
  - I always use an easy to guess password
  - Internet banking gives anyone access if a longer than expected password is entered
  - I do all of my internet banking using a PC at the local internet café
- Threats and attacks:
  - Attacker guesses my password
  - Attacker enters very long password
  - Attacker installs a keylogger to collect my password

Passive versus active threats and attacks

- Threats and attacks can be passive or active in nature
- Passive make no change to the system
    - E.g. guessing my password
- Active makes changes to the system
    - E.g. enters a very long password

Insider versus outsider threats and attacks

- Threats and attacks can come from inside or outside an organization
- Insider is usually user with legitimate access to a system but misuses it
  - I take money from my own account and claims it was stolen
- Outsider requires taking over the privileges of an insider
  - Attacker guesses my password, uses it to access my account and transfer money to themselves

Countermeasures

- **Countermeasures** are any means taken to try and prevent a successful attack. These may be technical or operational in nature.
- Consider Internet banking:
  - Train the user to choose harder to guess passwords.
  - Reject passwords that are too long.
  - Always use a computer that only I can access.
- **Unsuccessful countermeasure** leads to **successful attack** and a security property being violated
  - E.g. I lose money from my account (integrity property)

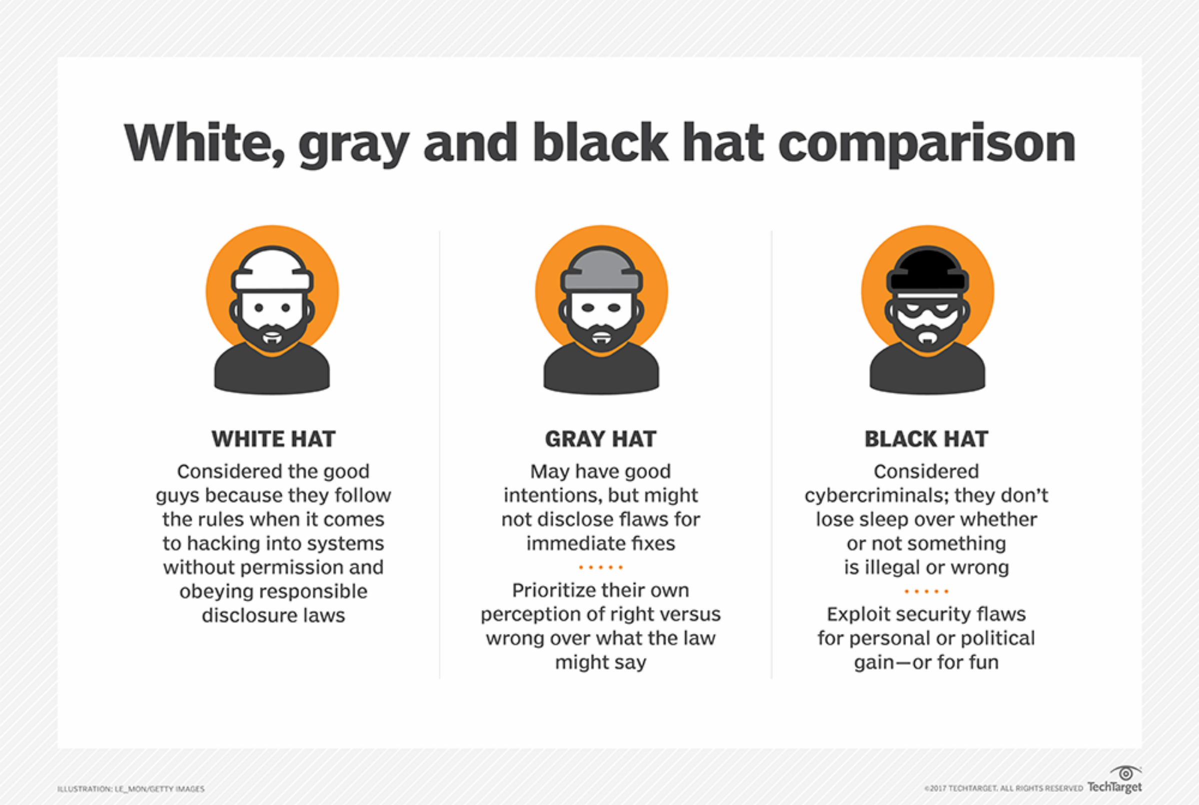
Why is it hard to get right?

1. Select defenses by considering **many** different attacks.
2. Only **one** attack needs to succeed.
3. Need to place defense **at the right point** in the system.
4. May rely on **keeping secrets** but also sharing them.
5. **Battle of wits** between attacker and defender.
6. People **don’t** realize value until security failure.
7. Security requires **constant** monitoring.
8. Often added as an **afterthought**.
9. Strong security viewed as making system **hard to use**.

PART III:
Who are the attackers?

Hackers (1995)

White, Grey and Black hat hackers



White, gray and black hat comparison

WHITE HAT

Considered the good guys because they follow the rules when it comes to hacking into systems without permission and obeying responsible disclosure laws

GRAY HAT

May have good intentions, but might not disclose flaws for immediate fixes

• • • • •

Prioritize their own perception of right versus wrong over what the law might say

BLACK HAT

Considered cybercriminals; they don't lose sleep over whether or not something is illegal or wrong

• • • • •

Exploit security flaws for personal or political gain—or for fun

ILLUSTRATION: LE_MON/GETTY IMAGES

https://www.techtarget.com/searchsecurity/definition/white-hat

White hat hacking in NZ context

- Abridged from https://2015.kiwicon.org/faq/

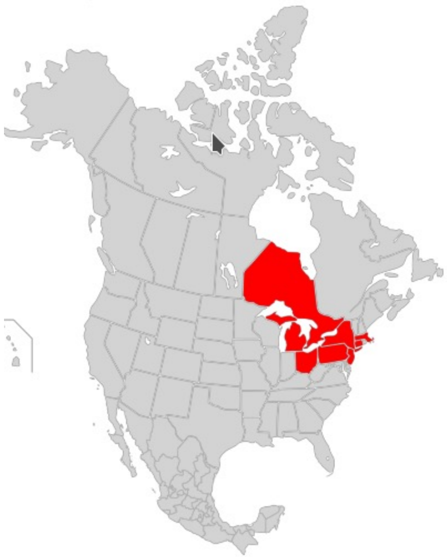
- I am not a lawyer but the New Zealand Crimes Act (section 248-254) documents laws criminalise certain acts involving computers.

- Most of these relate to the CIA properties being breached or enabling other people to do it (with intent).

- General rule #1: ask permission or hack your own system.
- General rule #2: just because you know how (maybe from this course) doesn't mean you should do it.
- General rule #3: its not motivation but what you did that counts

Ethical issues raised by grey hat hacking

- Unintended consequences:
  - Small changes can have big impacts
  - 2003 blackout on northwestern corridor due to software failure
  - Impossible to know the effect
- Morris worm 1988
  - Robert Morris exploited vulnerabilities in Unix to allow program to spread an count all computers on the Internet
  - Bug in his code caused all those computers to crash



Types of black hat hackers

- An adversary is a particular type of blackhat hacker.
- *Individual, group, organization or government that* ***conducts*** *or* ***has the intention*** *to conduct detrimental activities.*
- Lots of different types, with varying:
  - Ability
  - Resources
  - Motivations

Types of adversary: *Cyber criminals*

- Individuals or members of an organised crime group with a goal of financial reward
- Their activities may include:
  - Identity theft
  - Theft of financial credentials
  - Corporate espionage
  - Data theft
  - Data ransoming
- Typically they are young, often Eastern European, Russian, or southeast Asian hackers, who do business on the Web
- They meet in underground forums to trade tips and data and coordinate attacks

Types of adversary: *Activists*

- Are either individuals, usually working as insiders, or members of a larger group of outsider attackers, who are motivated by social or political causes
- Also know as hacktivists
  - Skill level is often quite low
- Aim of their attacks is often to promote and publicize their cause typically through:
  - Website defacement
  - Denial of service attacks
  - Theft and distribution of data that results in negative publicity or compromise of their targets

THE ASSET THEY ARE INTERESTED IN IS YOUR ATTENTION

Types of adversary: *State-sponsored organisations*

- Groups of hackers sponsored by governments to conduct espionage or sabotage activities
- Also known as Advanced Persistent Threats (APTs) due to the covert nature and persistence over extended periods involved with any attacks in this class
- Widespread nature and scope of these activities by a wide range of countries from China to the USA, UK, and their intelligence allies

PART IV:
Wrap up

What did we cover?

- What is cybersecurity?
- What are protecting against and how?
- Who are the attackers?

Thursday recap lecture

- Class representative election via GoSoapBox
- Overview of the lab and how to do it remotely
- Recent examples of cybersecurity failures - exercise